



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/734,962	12/11/2000	David Michael Kurn	20206-030 (P00-3014)	4932

7590 02/16/2005

Hewlett-Packard Company
Attn: Bill Streeter
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER

TESLOVICH, TAMARA

ART UNIT	PAPER NUMBER
----------	--------------

2137

DATE MAILED: 02/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/734,962

Applicant(s)

KURN ET AL.

Examiner

Tamara Teslovich

Art Unit

2137

— The MAILING DATE of this communication appears on the cover sheet with the correspondence address —
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on September 27, 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-31 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-31 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

This action is in response to the Amendment filed on September 27, 2004.

Claims 24, 25, and 28-31 have been amended and are herein considered.

Claims 1-31 are pending.

Response to Arguments

Applicant's arguments filed September 27, 2004 have been fully considered and are treated as follows:

Applicant's arguments with respect to Claims 27-31 have been fully considered but they are not persuasive.

Applicant's arguments with respect to Claims 1, 3-22, 25, and 26 have been fully considered but they are not persuasive.

Applicant's arguments with respect to Claims 2, 23, and 24 have been fully considered but they are not persuasive.

In reference to Claims 27-31, Applicant argues that the claims are not anticipated by Mitty et al., US Patent 6,199,052.

Applicant argues that Mitty et al. fails to teach or suggest steps c-e of claims 27-31, wherein steps c-e recites "(c) instantiating an application process on behalf of an end entity on the computer system, the end entity having credentials stored in the database; (d) requesting the Key Repository process for the credentials of the end entity

by the application process; and (e) if the Key Repository process authenticates the application process as having been pre-authorized to have the credentials, building an encrypted credentials file and providing the application process with the file and a password for the file.”

Applicant argues that Mitty et al. fails to teach or suggest a method of obtaining cryptographic credentials by an application running on a computer system as claimed in claims 27-31, arguing that there is no “instantiating an application process on behalf of an end entity on a computer system, the end entity have credentials stored in the database”. Examiner respectfully disagrees, bringing to the Applicant’s attention column 15 of Mitty et al. wherein “to send a request, an authorized user creates a S/MIME-3P structure ... [wherein] the inner and outer envelopes are encrypted with the intermediary’s public key ... [and] the waybill portion includes computer code indicating the verification transaction desired” (see col.15 lines 21-28). Examiner notes that the phrase “authorized user” refers to an end user whose credentials have already been collected, authorized and in the process, stored in the database”. Please refer to column 16 of Mitty et al. for clarification regarding the forming and use of S/MIME-3P packages, used by MIME agents in routing messages to and invoking appropriate software programs (see col.16 lines 10-13). Please note that the term “appropriate software” includes Applicant’s “application processes”.

Applicant also argues that Mitty et al. fails to teach or suggest “(e) if the Key Repository process authenticates the application process as having been pre-authorized to have the credentials, building an encrypted credentials file and providing

the application process with the file and a password for the file". Examiner draw's Applicant's attention to Mitty et al. columns 11 and 12 wherein after authorization, the combination of encrypted contents and key, encrypted with the user's public key, are combined to form the envelopedData structure and sent to the recipient (see col.11 line 66 thru col.12 line 12).

In reference to Claims 1, 3-22, 25, and 26, Applicant argues that the claims are not anticipated by Mitty et al., US Patent 6,199,052.

Applicant argues that Mitty et al. fails to teach or suggest an application that is "configured to query the Key Repository process for some or all of the sensitive information in the database". For purposes of examination, Examiner has chosen the following definition of 'application': "A program designed to assist in the performance of a specific task", quoted directly from the Fifth Edition of the Microsoft Computer Dictionary. Examiner would now like to bring to the Applicant's attention the MIME- and S/MIME-enabled email system residing on Mitty et al.'s server (see col.9 lines 53-56). Once invoked by the end user, this application is configured to create a S/MIME-3P structure including a waybill portion comprising computer code indicating desired verification transactions from the Intermediary Key Repository, including using the information from the structure and waybill portion to construct a search request of the database (see col.15 lines 21-32, 40-47; col.16 lines 11-13). Mitty et al.'s use of MIME agents and "application/x-smime3p" to "invoke the appropriate software" using "information supplied with the VR to construct a search request of the database" and

Applicant's "application configured to query the database" are considered equivalent for purposes of examination.

In reference to Claims 2, 23, and 24, Applicant argues that the claims are in condition for allowance given the comments above regarding Mitty et al., US Patent 6,199,052. However, Examiner maintains the abovementioned rejections in regards to Mitty et al. as well as those pertaining to Claims 2, 23, and 24.

Therefore, based on the above arguments, the Examiner maintains the rejections as set forth below.

Claim Rejections - 35 USC § 102

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claims 27-31 are rejected under 35 U.S.C. 102(b) as being anticipated by Mitty et al. (US Pat 6,199,052).

Regarding Claim 27, Mitty et al. teaches a method for obtaining cryptographic credentials by an application running on a computer system, the method comprising the steps of

- (a) providing a computer system having at least one server (col.9 lines 53-56);
- (b) instantiating a Key Repository process on the computer system, the Key

Repository process having a cryptographically protected database (col.4 lines 18-26; col.8 lines 34-40; col.9 lines 58-61);

(c) instantiating an application process on behalf of an end entity on the computer system, the end entity having credentials stored in the database (col.6 lines 24-33; col.11 lines 12-19);

(d) requesting the Key Repository process for the credentials of the end entity by the application process (col.2 lines 29-42); and

(e) if the Key Repository process authenticates the application process as having been pre-authorized to have the credentials (col.15 lines 6-20; col.19 lines 15-21), building an encrypted credentials file and providing the application process with the file and a password for the file (col.11 line 66 thru col.12 line 12).

Regarding Claim 28, Mitty et al. teaches instantiating a remote Key Repository process on a remote server (fig.1B; col.13 line 60 thru col.14 line 5).

Regarding Claim 29, Mitty et al. teaches instantiating a local agent on a remote server (fig.1B; col.13 line 60 thru col.14 line 5).

Regarding Claim 30, Mitty et al. teaches providing the Key Repository process with a remote agent interface; and linking the remote Key Repository process on the remote server to the Key Repository process via the remote agent interface (fig.1B; col.13 line 60 thru col.14 line 5).

Regarding Claim 31, Mitty et al. teaches providing the Key Repository process with an agent interface; and linking the local agent on the remote server to the Key Repository process via the agent interface (fig.1B; col.13 line 60 thru col.14 line 5).

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claims 1, 3-22, 25, and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ober et al. (US Pat 6,307,936), and further in view of Mitty et al. (US Pat 6,199,052).

Regarding Claim 1, Ober et al. teaches a method for providing scalable security services, comprising; instantiating at least one application on the computer system (col.3 lines 17-22; col.4 lines 53-54)); and instantiating a Key Repository process on the computer system, the Key Repository process configured to manage sensitive information in a database on the computer system using at least one master key (col.1 line 49 thru col.2 line 15; col.10 lines 30-35).

What Mitty et al. teaches that Ober et al. does not teach is validating and recording authorizations of specific applications to access sensitive information in the database, wherein each of the at least one application is configured to query the Key Repository process for some or all of the sensitive information in the database (col.2 lines 29-55; col.10 lines 28-55)), and in response to the query from a particular instance of the at least one application, provide to the particular instance of the at least one application the requested some or all of the sensitive information only if the Key Repository process authenticates the particular instance of the at least one application as being pre-authorized to receive the requested some or all of the sensitive information (col.15 lines 6-20; col.19 lines 15-21).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Ober et al.'s cryptographic key management scheme with Mitty et al.'s method of secure electronic transactions in order to provide a system that has privacy, authentication of participants, and non-repudiation, and is able to prevent eavesdroppers from being able to determine that a given sender is communicating with a given recipient (Mitty et al. col.2 lines 1-28).

Regarding Claim 3, the modified method of Ober et al. and Mitty et al. discloses the method of Claim 1, in addition Ober et al. teaches the Key Repository process is a centralized repository process for the at least one master key, as well as passwords, enterprise policy and policy decisions, authorizations to use enterprise credentials and

Art Unit: 2137

pre-authorization and authentication of the at least one application (col.6 lines 1-12; col.10 lines 30-35).

Regarding Claim 4, the modified method of Ober et al. and Mitty et al. discloses the method of Claim 1, in addition Ober et al. teaches at least one master key is configured as an encryption key that maintains the integrity of and protects the sensitive information (col.10 lines 9-35).

Claim 5 is substantially equivalent to Claim 1, therefore Claim 5 is rejected because of similar rationale.

Regarding Claim 6, the modified method of Ober et al. and Mitty et al. discloses the method of Claim 5, in addition Ober et al. teaches at least one master key maintains the integrity of and protects the sensitive information in the database (col.7 lines 21-24; col.7 lines 58-59).

Regarding Claim 7, the modified method of Ober et al. and Mitty et al. discloses the method of Claim 5, in addition Ober et al. teaches at least one master key provides privacy protection to the sensitive information on the database (col.10 lines 9-35).

Regarding Claim 8, the modified method of Ober et al. and Mitty et al. discloses the method of Claim 5, in addition Ober et al. teaches the sensitive information is a public key (col.4 lines 8-13).

Regarding Claim 9, the modified method of Ober et al. and Mitty et al. discloses the method of Claim 5, in addition Ober et al. teaches the sensitive information is a secret (col.2 lines 58-60; col.3 lines 34-45).

Regarding Claim 10, the modified method of Ober et al. and Mitty et al. discloses the method of Claim 5, in addition Ober et al. teaches the sensitive information is a private key (col.4 lines 14-23).

Regarding Claim 11, the modified method of Ober et al. and Mitty et al. discloses the method of Claim 5, in addition Ober et al. teaches the sensitive information is a symmetric key (col.9 lines 30-38).

Regarding Claim 12, the modified method of Ober et al. and Mitty et al. discloses the method of Claim 5, in addition Mitty et al. teaches the sensitive information is a certification authority certificate (col.4 line 62 thru col.5 line 25).

Regarding Claim 13, the modified method of Ober et al. and Mitty et al. discloses the method of Claim 5, in addition Ober teaches at least one master key are kept in physical memory (col.16 lines 40-51).

Regarding Claims 14 and 15, examiner takes official notice that non-swappable physical memories are well known in the art. It would have been obvious to one of ordinary skill in the art at the time of the invention to use non-swappable physical memory in order to allow the processor to focus on the tasks/jobs, such as tasks involving managing a key repository process and distributing sensitive information to authorized users, without wasting any allocated CPU time for swapping information in and out of memory.

Regarding Claim 15, the modified method of Ober et al. and Mitty et al. discloses the method of claim 5, in addition Ober et al. teaches the physical memory is protected (col.6 lines 10-12).

Regarding Claim 16, examiner takes official notice that virtual memories are well known in the art. It would have been obvious to one of ordinary skill in the art at the time of the invention to use virtual memories in order to allow a larger process to be executed by the CPU with a smaller amount of RAM.

Regarding Claim 17, the modified method of Ober et al. and Mitty et al. discloses the method of Claim 5, in addition Ober teaches at least one master key includes an integrity key configured to ensure the integrity of the sensitive information on the database (col.7 lines 21-23; col.7 lines 45-48).

Regarding Claim 18, the modified method of Ober et al. and Mitty et al. discloses the method of Claim 5, in addition Ober et al. teaches at least one master key includes a protection key configured to protect the sensitive information on the database (col.10 lines 55-63).

Regarding Claim 19, the modified method of Ober et al. and Mitty et al. discloses the method of Claim 5, in addition Mitty et al. teaches at least one application is a context-free server program (col.13 line 60 thru col.14 line 5).

Regarding Claim 20, the modified method of Ober et al. and Mitty et al. discloses the method of Claim 19, in addition Mitty et al. teaches at least one application is configured to retain context information across one or more instantiations of the at least one application (col.7 lines 56-65; col.14 line 66 thru col. 15 line 5).

Regarding Claim 21, the modified method of Ober et al. and Mitty et al. discloses the method of claim 20, in addition Mitty teaches the context information includes sensitive data (col.7 lines 56-65).

Regarding Claim 22, the modified method of Ober et al. and Mitty et al. discloses the method of Claim 19, in addition Mitty et al. teaches at least one application is configured to convey sensitive context information, by encrypting the information and then passing the information to a next instance of the at least one application (col.2 lines 29-55; col.11 line 60 thru col.12 line 12).

Regarding Claim 25, the modified method of Ober et al. and Mitty et al. discloses the method of Claim 9, in addition Mitty et al. teaches the secret is protected by a password (col.4 lines 24-26).

Regarding Claim 26, the modified method of Ober et al. and Mitty et al. discloses the method of Claim 25, in addition Mitty et al. teaches the secret can be updated in the absence of the password (col.2 lines 29- 55).

Claims 2, 23, and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified method of Ober et al. and Mitty et al., and further in view of Price (US pat 6,662,299).

Regarding Claim 2, the modified method of Ober et al. and Mitty et al. discloses the method of Claim 1 but fail to teach at least one master key is divided into a

predetermined number of portions each of which associated with a password, and wherein the sensitive information cannot be exposed without at least some or all of the predetermined number of passwords using a password-based private key encryption-decryption.

Price teaches at least one master key is divided into a predetermined number of portions each of which associated with a password, and wherein the sensitive information cannot be exposed without at least some or all of the predetermined number of passwords using a password-based private key encryption-decryption (col.1 lines 55-59; col.2 lines 49-59).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Ober et al. and Mitty et al.'s cryptographic key management scheme with Price's method for reconstructing an encryption key in order to discard the need for maintaining backup copies of passwords for users that can severely compromise the computer system security due to un-trusted system administrators (Price col.1 lines 47-64).

Regarding claim 23, the modified system of Ober et al. and Mitty et al. discloses the system of Claim 9, but fails to teach the secret is divided among a plurality of individuals. Price teaches the secret is divided among a plurality of individuals (col.1 lines 55-59; col.2 lines 49-59).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Ober et al. and Mitty et al.'s cryptographic key management

Art Unit: 2137

scheme with Price's method for reconstructing an encryption key in order to discard the need for maintaining backup copies of passwords for users that can severely compromise the computer system security due to un-trusted system administrators (Price col.1 lines 47-64).

Regarding Claim 24, the modified system of Ober et al., Mitty et al. and Price discloses the system of Claim 23, in addition Price teaches the integrity of the secret that is controlled by a first individual is increased by linking the secret to a second secret, the second secret is revealed only with the cooperation of all or a predetermined number of the plurality of individuals (col.1 lines 55-59; col.2 lines 49-59).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

Art Unit: 2137


the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571) 272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


Tamara Teslovich


ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER

February 11, 2005